PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PE17234PC00	FOR FURTHER ACTION See Form PCT/IPEA/416	
International application No. PCT/SE2003/000664	International filing date *(day/month/year)* 25-04-2003	Priority date *(day/month/year)* 15-08-2002
International Patent Classification (IPC) or national classification and IPC H04L 12/14, H04Q 7/32, H04Q 7/38		
Applicant Telefonaktiebolaget LM Ericsson (publ) et al		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 8 sheets, as follows:
      ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) _____, containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).
4. This report contains indications relating to the following items:
   - ☒ Box No. I Basis of the report
   - ☐ Box No. II Priority
   - ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - ☐ Box No. IV Lack of unity of invention
   - ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - ☒ Box No. VI Certain documents cited
   - ☐ Box No. VII Certain defects in the international application
   - ☐ Box No. VIII Certain observations on the international application

Date of submission of the demand	Date of completion of this report
23-01-2004	04-11-2004
Name and mailing address of the IPEA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. +46 8 667 72 88	Authorized officer Elisabet Åselius/MN Telephone No. +46 8 782 25 00

Form PCT/IPEA/409 (cover sheet) (January 2004)

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International Application No.
PCT/SE2003/000664

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This report is based on a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of:

☐ international search (under Rules 12.3 and 23.1(b))
☐ publication of the international application (under Rule 12.4)
☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):*

☐ the international application as originally filed/furnished

☒ the description:

pages 1-48 as originally filed/furnished
pages* _____ received by this Authority on _____
pages* _____ received by this Authority on _____

☒ the claims:

pages _____ as originally filed/furnished
pages* _____ as amended (together with any statement) under Article 19
pages* 49-56 received by this Authority on 2004-07-13
pages* _____ received by this Authority on _____

☒ the drawings:

pages 1-11 as originally filed/furnished
pages* _____ received by this Authority on _____
pages* _____ received by this Authority on _____

☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/figs _____
☐ the sequence listing *(specify)*: _____
☐ any table(s) related to the sequence listing *(specify)*: _____

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/figs _____
☐ the sequence listing *(specify)*: _____
☐ any table(s) related to the sequence listing *(specify)*: _____

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International Application No.
PCT/SE2003/000664

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-45	YES
	Claims		NO
Inventive step (IS)	Claims	1-45	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-45	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

The claimed invention relates to a method of monitoring client usage of digital content provided by a content provider, to ensure correct billing and that the content provider is not cheated.

Documents cited in the International Search Report:

D1: US 20010053223 A1

D2: WO 0198956 A1

D3: WO 0237822

D4: WO 0231760

D5: WO 0219593

D1 reveals a method of monitoring client-usage of digital content (or a service) provided by a content provider to a client system over a network, (abstract). Usage information concerning the usage of said digital content (or service) is logged, (paragraph 0009) individually, (paragraph 0008), for each usage to be monitored. A security operation to enable identification of at least one of an account and an individual is performed, (paragraphs 0015-0018).

An authentication of the usage information is performed, (paragraph 0015), and part of the authentication comprises a signing key, encrypting by encryption key or appending an authentication tag, (claims 2-8). The usage information in question comprises a representation, and quality and time information, (paragraph 0204; figs. 13-16). It also comprises bandwidth and payment information.

Usage information is forwarded to an external trusted party, (paragraphs 0014, 0016-0018).

D2 also discloses a method of monitoring client-usage of digital content, (p.4 line 3-p.6 line 13; p.15 lines 26-30; p.16 lines 1-12; abstract). .../...

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Box V

Documents D3 and D4 both reveal how logs are stored in tamper-resistant devices, associated with the client system, (D3: p.4 line 29-p.5 line 8; D4: p.2 line 26-p.3 line 19).

D5 deals with service provider-independent end-user authentication.

Neither D1 nor D2 nor D3-D5 reveals the generation of information concerning the actual rendering of ordered, received and subsequently decrypted digital content, which the claimed invention does. This information is generated either during the content rendering process or when it has been completed. In this way users are deterred from repudiating the rendering of the digital content.

Thus, the claimed invention fulfils the requirements of novelty, inventive step and industrial applicability.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International Application No.
PCT/SE2003/000664

Box No. VI Certain documents cited

1. Certain published documents (Rule 70.10)

Application No. Patent No.	Publication date *(day/month/year)*	Filing date *(day/month/year)*	Priority date (valid claim) *(day/month/year)*
WO 03003654 A1	09.01.2003	27.06.2002	29.06.2001

2. Non-written disclosures (Rule 70.9)

Kind of non-written disclosure	Date of non-written disclosure *(day/month/year)*	Date of written disclosure referring to non-written disclosure *(day/month/year)*

CLAIMS

1. A method of monitoring client-usage of digital content provided by a content provider (30) to a client system (10) over a network (40), said method including the step of:

- logging information concerning the actual rendering of said digital content individually for each rendering to be monitored; and
- performing a security operation to enable identification of at least one of an account and an individual for linking said usage information thereto.

2. The method according to claim 1, further comprising the step of decrypting said digital content prior the rendering of said digital content.

3. The method according to claim 1, wherein said step of performing a security operation comprises the step of performing at least part of an authentication of said information.

4. The method according to claim 1, wherein said information is maintained in a log (175) in said client system (10), and said step of performing a security operation comprises the step of storing said log (175) in a tamper-resistant environment associated with said client system (10).

5. The method according to claim 1, wherein said information comprises a representation (172-1) of said client-rendered digital content and rendering quality information (172-2).

6. The method according to claim 5, wherein said quality information (172-2) comprises at least one of:

- bandwidth of said rendered digital content;
- sample rate of said digital content;

- data compression of said digital content;
- resolution of said used digital content;
- time information (172-N) related to rendering of said digital content; and
- information of any disruptions during the rendering of said digital content.

7. The method according to claim 1, wherein said information comprises at least one of:

- identification of a content-usage device (300);
- information on payment of said digital content;
- time information (172-N) related to rendering of said digital content;
- time information related to transmittal of said digital content from said content provider (30) to said client system (10); and
- time information related to reception of said digital content by said client system (10).

8. The method according to claim 1, wherein said logging step comprises the steps of:

- tamper-resistantly generating said information; and
- storing said information as a log entry (172) in a user-tamper-resistant log (170; 175; 175-1, 175-2).

9. The method according to claim 1, wherein said logging step comprises the step of generating said information during said digital content rendering or after said digital content rendering.

10. The method according to claim 1, further comprising the step of forwarding said information from said client system (10) to an external trusted party for storage therein as log entry (172) in a usage log (170).

11. The method according to claim 1, wherein said digital content is provided as streaming data and said digital data is used by said client system (10), said step of logging information comprises the step of for each on-going client-usage of streaming data, intermittently logging information during said client-usage.

12. The method according to claim 11, further comprising the step of intermittently forwarding said intermittently logged information to said content provider (30) for confirming reception and rendering of the data.

13. The method according to claim 12, wherein said information is included into receive reports associated with the report mechanism of the streaming protocol used for streaming said data.

14. Client system (10) capable of using digital content provided by a content provider (30) over a network (40), said content-using client system (10) comprising:

- logging agent (150) for logging information concerning the actual rendering of said digital content individually for each one of a set of client-renderings; and
- means (160; 460) for performing a security operation to enable identification of at least one of an account and an individual for linking said information thereto.

15. The client system according to claim 14, further comprising means (130; 430) for decrypting said digital content prior the rendering of said digital content.

16. The client system according to claim 14, wherein said security operation performing means (160; 460) is configured for performing at least part of an authentication of said information.

17. The client system according to claim 14, wherein said information is maintained in a log (175) in said client system (10), and said security operation

performing means is configured for storing said log (175) in a tamper-resistant environment associated with said client system (10).

18. The client system according to claim 14, wherein said information comprises a representation (172-1) of said client-rendered digital content and rendering quality information (172-2).

19. The client system according to claim 14, wherein said logging agent (150) comprises:

- means (152) for tamper-resistantly generating said information; and
- means (154; 156) for storing said information as a log entry (172) in a log (170; 175).

20. The client system according to claim 14, wherein said logging agent (150) comprises means (152) for generating said information during or after rendering of said digital content.

21. The client system according to claim 14, wherein said logging agent (175) further comprises means (156) for forwarding said information to an external trusted party for storage therein as a log entry (172) in a log (170).

22. The client system according to claim 14, further comprising:

- a rendering device (300) adapted for rendering said provided digital content; and
- a first digital rights management (DRM) agent (130; 330), at least partly implemented in said rendering device (300), having functionality for enabling rendering of said digital content.

23. The client system according to claim 22, further comprising:

- a second DRM agent (230; 430) implemented in said client system (100), having functionality for enabling reception of said digital content from said content provider (30); and

- means (210; 310; 410) for communication between said first DRM agent (330) and said second DRM agent (230; 430), said first DRM agent (330) comprising means for transferring a first control signal associated with said information to said second DRM agent (230; 430) and said second DRM agent (230; 430) comprises means for processing signal data associated with said first control signal to generate a second control signal, and means for sending said second control signal to said first DRM agent (330) for controlling the digital-content usage process.

24. The client system according to claim 14, further comprising a tamper resistant module, in which said logging agent (150) is implemented.

25. The client system according to claim 24, wherein said tamper resistant module is a subscriber identity module (400).

26. The client system according to claim 25, wherein said logging agent (150) is at least partly implemented as an application in an application environment (490) provided by an application toolkit associated with said subscriber identity module (400).

27. The client system according to claim 26, wherein said logging agent application is downloaded into said subscriber identity module (400) over said network (40) from a network service provider (20; 30) associated with said subscriber identity module (400).

28. The client system according to claim 14, wherein said digital content is provided as streaming data and said client system (10) comprises means (300) for rendering said streaming data, and said logging agent (150) is configured to, for each

on-going client-rendering of streaming data, intermittently generate information during said client-rendering.

29. The client system according to claim 28, further comprising means (156) for intermittently forwarding said intermittently generated information to said content provider (30) for confirming reception and rendering of the data.

30. The client system according to claim 29, wherein said information is included into receive reports associated with the report mechanism of the streaming protocol used for streaming said data.

31. A digital rights management system for assisting in the management of digital content provided to a client system (10) over a network (40), said management system comprising:

- means (22) for receiving, for each one of a set of renderings of said digital content by said client system (10), information over said network (40), said information concerning the rendering of said digital content and originating from said client system (10); and
- means (180) for storing said information in a log (170; 175)), said information being subjected to at least part of an authentication procedure to enable identification of at least one of an account and an individual for linking said information thereto.

32. The system according to claim 31, further comprising means (22) for downloading a logging agent (150) into said client system (10), said logging agent (150) being operable, when executed in said client system (10), for generating, for each one of said client-renderings, information concerning the rendering of said digital content and forwarding said information to said storing means (180).

33. The system according to claim 31, wherein said digital content providing means (32) is configured for providing said digital content to said client system (10) as streaming data, said system further comprising means (32) for terminating the flow of streaming data to said client system (10) if no information has been received during a predetermined period of time.

34. The system according to claim 31, wherein said system is implemented in a network operator node.

35. A tamper-resistant device (400) adapted for cooperation with a client system (10) capable of rendering digital content provided by a content provider (30) over a network (40), said tamper-resistant device (400) comprising:

- logging agent (150) for logging information concerning the rendering of said digital content individually for each one of a set of client-renderings, said tamper-resistant device (400) being associated with means (160; 460) for performing a security operation to enable identification of at least one of an account and an individual for linking said information thereto.

36. The device according to claim 35, further comprising means (430) for decrypting said digital content prior to the rendering of said digital content.

37. The device according to claim 35, wherein said security operation performing means (160; 460) is provided in said tamper-resistant device (400) for performing at least part of authentication of said information.

38. The device according to claim 35, wherein said information is maintained in a log (175) in said tamper-resistant device (400).

39. The device according to claim 35, wherein said logging agent (150) comprises means (152) for generating said information during or after rendering of said digital content.

40. The device according to claim 35, wherein said logging agent (150) further comprises means (156) for forwarding said information to an external trusted party for storage therein as a log entry (172) in a log (170).

41. The device according to claim 35, wherein said tamper-resistant device (400) is a subscriber identity module.

42. The device according to claim 41, wherein said logging agent (150) is at least partly implemented as an application in an application environment (490) provided by an application toolkit associated with said subscriber identity module (400).

43. The device according to claim 35, wherein said logging agent application is downloaded into said subscriber identity module (400) over said network (40) from a network service provider (20; 30) associated with said subscriber identity module (400).

44. The device according to claim 35, further comprising means for downloading upgrades of said logging agent (150).

45. A method of monitoring client-usage of a service provided by a service provider (30) to a client system (10), said method including the step of:

- logging usage information concerning the actual usage of said service individually for each usage to be monitored; and
- performing a security operation to enable identification of at least one of an account and an individual for linking said usage information thereto.